Cyber Horizon

INCIDENT RESPONSE REPORT

From cloud identity compromise to on-prem ransomware

Veltaro SA

Sample incident response report. Composite, anonymised scenario

Prepared by **Cyber Horizon SRL, Aurélien Cuvelier, GSE #433**

Date **12 November 2026 · Version 1.0**

Classification **TLP:CLEAR**

SAMPLE - EXCERPT
cyberhorizon.be · full report on request

2. Executive summary

In brief. An attacker used the stolen password of Veltaro's IT provider to take control of its Microsoft 365 tenant, then built two routes into the datacentre, took over the domain, stole about 140 GB of data and encrypted 38 servers and the main backups on 3 October 2026.

Impact: six days of disruption, seven days of data lost, a personal data breach notified to the authorities. The customer platform was not affected and no ransom was paid.

Decisions needed: fund the priority 1 actions of section 8 within 30 days, starting with MFA for all administrators and third parties and alerting on identity changes.

On Saturday 3 October 2026 at 06:40, Veltaro's on-call IT engineer could not reach the internal services during the morning checks and found that the company's on-premises servers were unavailable and that ransom notes had been left on the virtualisation platform. Cyber Horizon was engaged at 09:30 the same day to lead containment, investigation and recovery.

The attack started in the cloud, ten weeks earlier. On 21 July, an attacker signed in to Veltaro's Microsoft 365 tenant with the account of its managed IT provider, Quadrix IT Services. That account held Global Administrator rights and its password had been stolen by information-stealing malware on a Quadrix workstation in early June. It had no multi-factor authentication method registered: when Microsoft asked for one at the first sign-in, the attacker simply registered their own authenticator app. After three weeks of short validation sign-ins, the attacker set up durable access: a certificate on an existing enterprise application, a backdoor account disguised as an emergency access account, and a registered device.

The attacker then built two bridges to the internal network. First, they created a virtual machine in Veltaro's Azure subscription and attached it to the network that is linked to the on-premises datacentre by a site-to-site VPN. Second, they used the IT helpdesk mailbox to send an internal phishing email about a "VPN certificate renewal", and harvested the credentials of six employees, including an IT administrator whose VPN access did not require MFA.

Once inside, the attacker took the Active Directory domain in two days. Credentials dumped from three servers, a service account vulnerable to Kerberoasting and one password reused on three service and administrator accounts led to the managed provider's Domain Admin account, then to a DCSync of the `krbtgt` account on 22 August. The attacker installed a reverse proxy and remote-access software for persistence, then went silent for four weeks.

A second phase began on 22 September. Activity resumed through the same reverse proxy, with different tools and working hours, which points to the access being handed over to a ransomware affiliate. About 140 GB of contracts, payroll, customer and strategy documents were archived and sent out through the Azure VM. On the night of 2 to 3 October, the attacker abused the hypervisors' Active Directory integration to obtain full rights on both ESXi hosts, encrypted every virtual machine disk, and encrypted the backup repository.

Recovery was possible without paying. A weekly offline copy of the backups, stored outside the domain, had not been reached. Core services were restored in six days. The attackers' claims about stolen data were checked against the exfiltration evidence, and the ransom was not paid.

SAMPLE · EXCERPT
cyber-horizon.be · for training purposes

This is an excerpt

You have just read the cover and the executive summary of a 30-page sample incident response report. The scenario is fictitious and fully anonymised, but the report follows the exact structure and level of detail of a real Cyber Horizon engagement.

What the full report contains

- Sources analysed and limitations
- Full attack timeline, from the first cloud sign-in to the encryption
- MITRE ATT&CK mapping of every phase
- Affected systems, accounts and indicators of compromise
- Technical analysis of each phase, with evidence
- Threat assessment and where the chain could have been broken

And what the client does next

- Eight root causes, each linked to the actions that fix it
- What was already done during the response
- Notifications and legal follow-up (GDPR, NIS2)
- Prioritised recommendations at 30 days, 90 days and 6 months
- Active Directory and infrastructure findings

Request the full 30-page report

Send a short request from your work email address and I will send you the complete report.

Email info@cyberhorizon.be
Web cyberhorizon.be/#contact
Phone +32 491 54 92 44